

DEMONSTRATED CASES OF INSECURITY IN CONTROL SYSTEMS

Wesley McGrew

Ray Vaughn

Mississippi State University

Critical Infrastructure Protection Center

Report Documentation Page			Form Approved OMB No. 0704-0188	
<p>Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p>				
1. REPORT DATE AUG 2010	2. REPORT TYPE	3. DATES COVERED 00-00-2010 to 00-00-2010		
4. TITLE AND SUBTITLE Demonstrated Cases of Insecurity in Control Systems			5a. CONTRACT NUMBER	
			5b. GRANT NUMBER	
			5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)			5d. PROJECT NUMBER	
			5e. TASK NUMBER	
			5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Mississippi State University,Critical Infrastructure Protection Center, Mississippi State, MS, 39762			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSOR/MONITOR'S ACRONYM(S)	
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited				
13. SUPPLEMENTARY NOTES Presented at the 22nd Systems and Software Technology Conference (SSTC), 26-29 April 2010, Salt Lake City, UT. Sponsored in part by the USAF. U.S. Government or Federal Rights License				
14. ABSTRACT				
15. SUBJECT TERMS				
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 15
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified		

Vulnerabilities in HMI Software

- GE Fanuc Proficy iFIX 4.5/5.0
- Insecure storage of passwords
- Authentication bypass
- Allows those with access to escalate privileges on the SCADA system
 - Lower-level personnel with physical access
 - Remote attackers with access via other/mainstream exploits

Case Study: iFIX



GE Fanuc
Intelligent Platforms



Proficy HMI/SCADA – iFIX 5.0



©2008 GE Fanuc Intelligent Platforms, Inc. All rights reserved.
†Trademark of GE Fanuc Intelligent Platforms, Inc. All other brands or names are property of their respective holders.

US Cert Vulnerability Announcement #310355

<http://www.nerc.com/fileUploads/File/Events%20Analysis/A-2009-02-10-01.pdf>

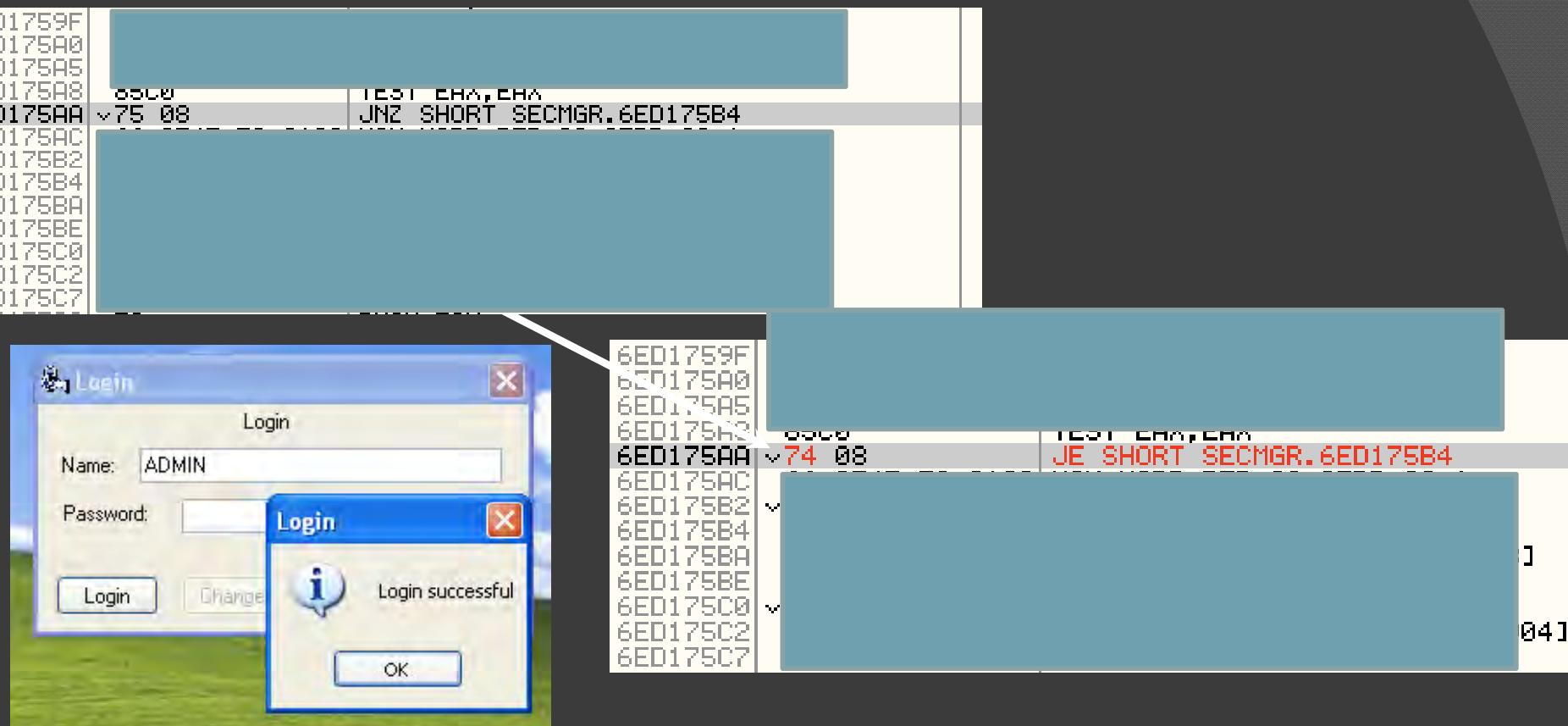
Insecure Password Storage

0000000:	2cd1	2df9	4763	087f	86d1	d4f8	45d6	0990	. .-. Gc.....E...
0000010:	41d8	dfba	fbe0	a235	088e	0ab3	6f63	3c18	A.....5....oc<.
0000020:	812e	d881	b908	7d4b	7ab9	33cd	e1de	9a15}Kz.3.....
0000030:	f4d0	2c30	621c	f857	6019	dea3	4a11	f6fd	.,,Ob..W`...J...
0000040:	7d28	05e2	cc4f	772c	8977	a92b	4cca	4677	}(...Ow,,.w.+L.Fw
0000050:	9353	fec4	bd81	793a	9ac3	5b35	e604	e26d	.S.....y:...[5...m
0000060:	5542	10ea	8b0d	5228	a408	2974	9da2	d3a3	UB.....R(..)t....
0000070:	28a4	7c59	04ed	dbc6	6fee	8c9f	cdb1	65ef	(. Y....o.....e.

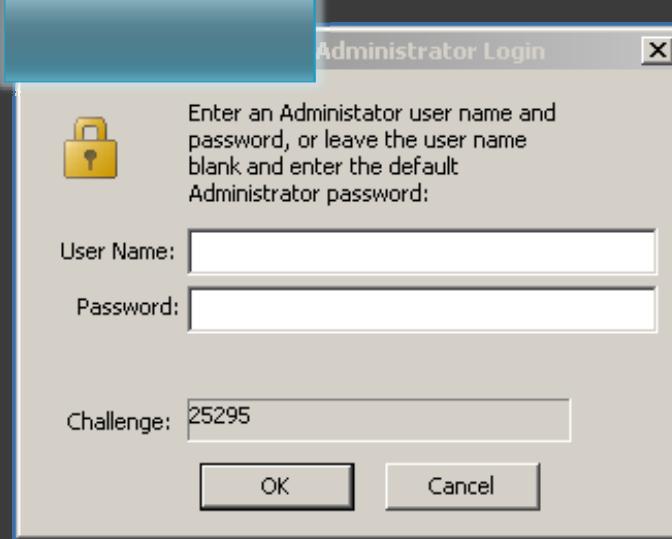
User's Full Name	bash-3.2\$./ifixpassdump.py XTCOMPAT.UTL		
Password	User	Password	Full Name
<hr/>			
Username	ADMIN	ADMINADMIN888	SYSTEM ADMINISTRATOR
	GCLARK	GC	GEORGE CLARK?5??
	GUEST	GUEST	GUEST ADMINISTRATOR
	LJONES	MYPASS	LAURA JONES?5??
	PSMITH	PSMITH1978	PETER SMITHA?5??
	TWHITE	J174ERT	THOMAS WHITE?5??

- User information/password is XOR'd with a static key and saved to XTCOMPAT.UTL
- User credentials can be recovered from this file

Authentication Bypass



- Authentication is performed by a process running as the current Windows user
- A copy of the login program and security DLL can be made, modified, and used to log in as any user with any incorrect password
 - Single-byte patch to the DLL to branch differently after comparing passwords



More violations of security principles in HMI software...

A screenshot showing a second instance of the "Administrator Login" dialog box, identical to the one above, displayed over a Windows desktop environment. The desktop includes a taskbar with icons for File Explorer, Task View, and Start. A file explorer window is open, showing a tree view with "NEW GROUP" expanded, revealing "NEW GROUP1" and "NEW GROUP2". To the right of the file explorer is a list of users: ADMIN, OPERATOR, USER2, and USER3.

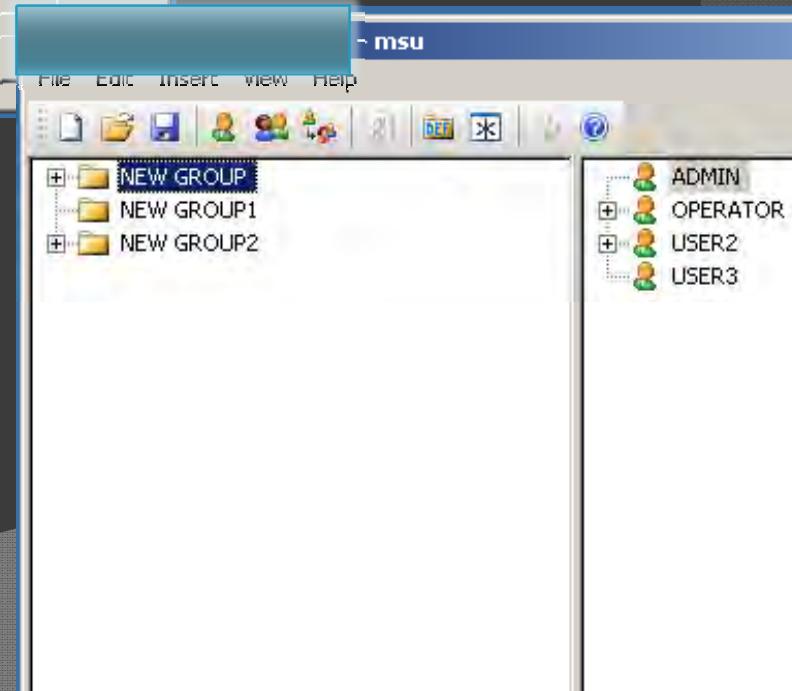
Locked-out customers may call support to get a response to the “Challenge” Field



An attacker can discover
(on their own time/systems)
the algorithm used for challenge
responses

Result:

Attacker is logged into security
server as the default admin
account. Can grant/deny
permissions, add/remove
users

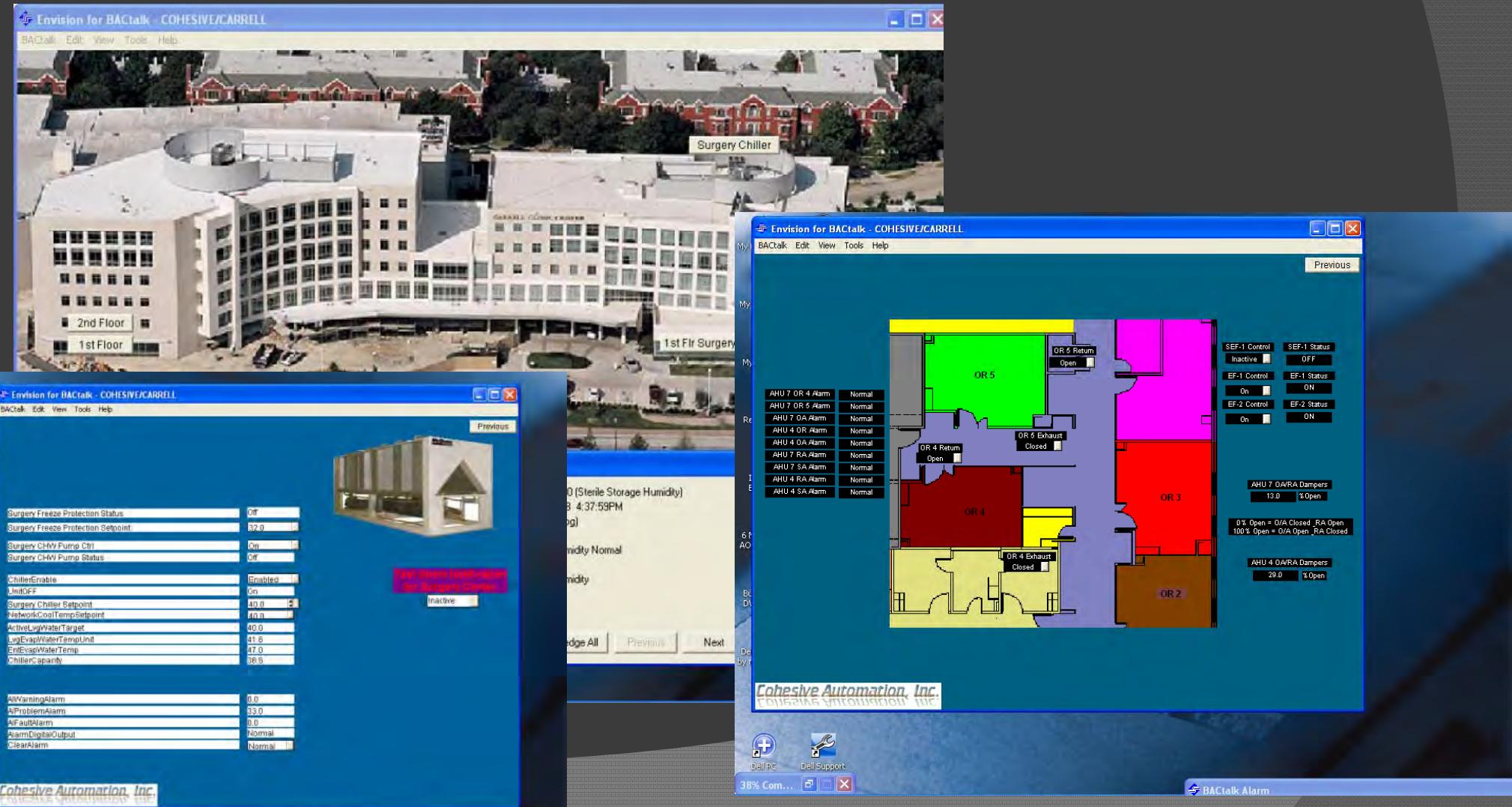


Response is first 8 characters
of MD4(challenge)

Easily calculated on a
mobile device

Real-World HMI Security Incident

Texas Hospital Control System Incident – late June to early July 2009



SCADA Communications

Vulnerabilities

- PLC Radios
 - Freewave 900 MHz
 - 902-928 ISM Unlicensed band
 - Point to Multi-Point serial over wireless
- Attacks
 - Scanning for radios
 - NMAP-like capability for PLC radios
 - Eavesdropping
 - Denial of Service

Student Researcher: Bradley Reaves

Discovery Scans

- Determines:
 - Existence of network
 - Access Control (Network Identifier or Serial Number)
- Network Identifier Scan
 - 12,288 combinations
 - Scan time: 6.4 secs/combo
 - Max runtime: 21.76 hours

Discovery Scans

◎Serial Number Scan

- 96,000 Combinations
- Scan Time: 1.7 secs/combo
- Max runtime: 45.5 hours

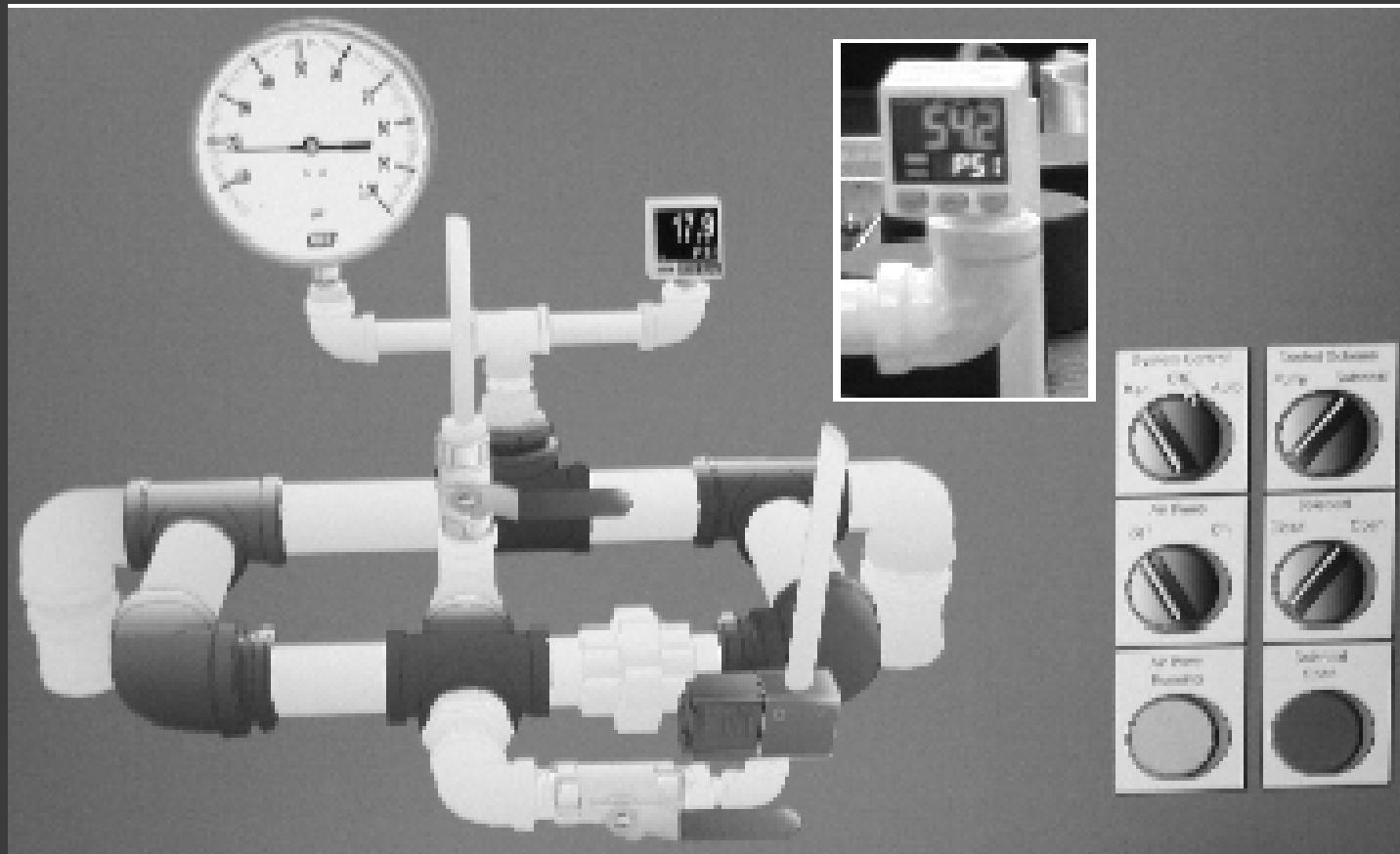
Infiltration Scans

- Seeking a continuous, unbroken connection
- Need Frequency Settings
- 539,400 Legal Combinations
- Can scan at 12s / combination
- Max time: 75 days
- +2.25 days to eliminate false positives

Denial of Service

- If our rogue slave transmits continuously, nothing else gets through.
 - `cat /dev/urandom > /dev/ttys0` brings the whole system down
- This can be **deadly** in a PCS system
- This attack mirrors symptoms seen in the Bellingham incident

Denial of Service



Conclusions

- We (our lab, vendors, and infrastructure) have made significant progress in SCADA security.
 - Lots of vulnerabilities
 - Potential for serious incidents
 - Lack of applied security principles
- We are heading in the right direction
 - Finding vulnerabilities
 - Averted at least one control system incident
 - Mapping out where these principles can be applied, and educating others